FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellee*, v. DAREN W. PHILLIPS, *Defendant-Appellant.*	No. 20-10304 D.C. No. 3:18-cr-00101- MMD-WGC-1 OPINION

Appeal from the United States District Court
for the District of Nevada
Miranda M. Du, Chief District Judge, Presiding

Argued and Submitted November 15, 2021
San Francisco, California

Filed April 29, 2022

Before: Richard A. Paez and Michelle T. Friedland, Circuit Judges, and Edward R. Korman,* District Judge.

Opinion by Judge Korman

* The Honorable Edward R. Korman, United States District Judge for the Eastern District of New York, sitting by designation.

SUMMARY[**]

Criminal Law

The panel affirmed a judgment of conviction in a case in which Daren Phillips entered a conditional guilty plea to possession of child pornography, reserving the right to appeal the denial of his motion to suppress evidence found on his laptop computer.

After calling off her engagement to Phillips, Amanda Windes discovered child pornography on his computer, which she then brought to the Washoe County Sheriff's Office. While Windes was there, Detective Gregory Sawyer asked her to show him only images that she had already viewed when she had accessed the laptop by herself. Windes complied with that request.

Phillips moved to suppress on the ground that, because Sawyer directed Windes to access the computer without Phillips's permission to show Sawyer what she had already seen, Windes's search of the computer at the sheriff's office was an unlawful law-enforcement search.

Because the U.S. Attorney does not dispute Phillips's assertion that Windes acted as a state agent when she accessed the computer at the sheriff's office, the panel assumed that this was a government search.

But applying *United States v. Jacobsen*, 466 U.S. 109 (1984), and *United States v. Bowman*, 215 F.3d 951 (9th Cir.

[**] This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

2000), the panel held that the search was permissible because, as the parties agree, when Windes accessed the child pornography on Phillips's computer at the sheriff's office, she merely mimicked her earlier private search. The panel rejected Phillips's argument that *Jacobsen* imposes requirements tied to law enforcement's subjective knowledge. The panel distinguished *United States v. Young*, 573 F.3d 711 (9th Cir. 2009), on the ground that this case does not involve a warrantless entry into a home or its equivalent. The panel rejected Phillips's argument that the "common-law trespassory test" set forth in *United States v. Jones*, 565 U.S. 400 (2012), requires suppression in this case.

Noting that in light of Phillips's valid appeal waiver he may argue on appeal only that the supervised-release conditions he challenges exceed the permissible statutory penalty or violate the Constitution, the panel wrote that this court's precedents establish the legality of all the challenged conditions (risk notification, prohibiting access to sexually explicit conduct material involving adults, polygraph testing).

COUNSEL

Aarin E. Kevorkian (argued), Assistant Federal Public Defender; Rene L. Valladares, Federal Public Defender; Office of the Federal Public Defender, Las Vegas, Nevada; for Defendant-Appellant.

William R. Reed (argued), Assistant United States Attorney; Elizabeth O. White, Appellate Chief; Christopher Chiou, Acting United States Attorney; United States Attorney's Office, Reno, Nevada; for Plaintiff-Appellee.

OPINION

KORMAN, District Judge:

In early 2018, Amanda Windes decided to call off her engagement to Daren Phillips. She believed Phillips had been lying to her about his alcohol use and financial troubles. She had also found "very inappropriate" text messages between Phillips and other women. Windes informed Phillips that he was no longer welcome in the house they shared. Two days later Phillips acknowledged that he needed help for his alcoholism, and Windes drove Phillips to a hospital, which arranged for a one-month stay at a residential treatment center. Windes had custody of many of Phillips's possessions while he was away, including his laptop computer. Windes was contacted by Phillips's ex-wife, Kelly Greek, who was worried about how Phillips would pay child support while he was in treatment. Greek also told Windes that she suspected that Phillips had watched child pornography and that Phillips may have been sexually interested in a friend of Greek's daughter.

Windes decided to examine Phillips's laptop. She said that her primary purpose was to examine his financial documents but that she also wanted to see if Phillips had been contacting other women and whether he had been viewing child pornography. She explained that she was also trying "to determine what other issues there w[ere] on top of [Phillips's] alcohol problem for the safety of my children and myself." The laptop was password protected, and Windes first tried the password for Phillips's Netflix account, which he had given to her. That password didn't work, so Windes clicked on the laptop's "forgot your password" function, which prompted her to answer Phillips's security questions. She successfully guessed the answers to those questions, which allowed her to send a

temporary password to her own email account. She was then able to reset the password and enter Phillips's computer.

As Windes browsed Phillips's computer, she came across a folder entitled "phone." She saw that it was several hundred megabytes in size and opened the folder. The folder displayed the names of all the files in the folder and their associated "thumbnail illustration[s]" (a small photo which indicated what each file contained). There were thousands of such thumbnail illustrations in the folder. They included "pictures of infants and all of their exposed genitalia" and "images of young females" who were "very scantily clad and [were in] extremely sexually provocative poses." As she scrolled down through the folder, she saw that many of the file names indicated how old the children were (from infants to teenagers). Windes saw that this "phone" folder contained *only* child pornography. She testified that the images were "highly graphic" and left her "disgusted." She "felt law enforcement needed to further investigate."

Windes first took the laptop to Police Services at the University of Nevada (where she worked) and told them only that she had a computer that she needed somebody to look at. Police Services told her to take the computer to the Washoe County Sheriff's Office ("sheriff's office") because it did not belong to the university. At the sheriff's office, Windes told the front desk deputy that she had a computer that she suspected contained a significant amount of child pornography. She was then interviewed by Detective Arick Dickson for about two-and-a-half hours. Windes told Dickson what she had found and how she had accessed the computer. She described in detail many of the thumbnail images of child pornography she had seen. She also relayed to Dickson her "concerns for . . . [her] children's safety,

especially due to the nature of the material on Phillips'[s] laptop."

Dickson then brought in Detective Gregory Sawyer, who asked Windes to show him only images that she had already viewed when she had accessed the laptop by herself. Windes and Sawyer testified—and the district court found—that Windes complied with that request and showed the detectives only the thumbnail images and accompanying file names she had previously seen while scrolling through the "phone" folder. Only Windes operated the computer while she showed Sawyer the images. Sawyer recognized some of the thumbnail images from prior child pornography investigations. Sawyer then seized the laptop and applied for and obtained a search warrant. The application included a brief written description of two thumbnail images that Windes had shown him and the associated file names. A subsequent forensic search of the laptop found over 4,750 images of child pornography and 538 child pornography videos.

Phillips was indicted for one count of transportation of child pornography, in violation of 18 U.S.C. § 2252A(a)(l), and one count of possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). He moved to suppress the evidence from the laptop on the ground that, because Sawyer directed Windes to access Phillips's computer without his permission to show Sawyer what she had already seen, Windes's search of the computer at the sheriff's office was an unlawful law-enforcement search. After holding a hearing, the district judge denied the motion.

Phillips then entered a conditional guilty plea to one count of possessing child pornography, reserving the right to appeal the denial of his motion to suppress. Phillips was sentenced to 63 months' incarceration and 20 years of

supervised release subject to certain conditions that he also challenges on appeal.

DISCUSSION

The Supreme Court has long held that it does not violate the Fourth Amendment for a law enforcement officer to accept and use evidence that a private party discovers pursuant to its own private search, even if that private search was unlawful. *See Burdeau v. McDowell*, 256 U.S. 465, 475–76 (1921); *Coolidge v. New Hampshire*, 403 U.S. 443, 485–90 (1971). This rule is based on the principle that "[t]he Fourth Amendment[']s]protection against unlawful searches and seizures . . . applies to governmental action" and "was not intended to be a limitation upon other than governmental agencies." *Burdeau*, 256 U.S. at 475. Moreover, "the consequences of *Burdeau* do not offend the more modern rationale of the Fourth Amendment exclusionary rule . . . [which] is most often explained on grounds of deterrence." 1 Wayne R. LaFave, Search & Seizure § 1.8(a) (6th ed. 2021). Specifically, "extension of the exclusionary rule to all private illegal searches for purposes of deterrence would be difficult to justify" because "the private searcher . . . is often motivated by reasons independent of a desire to secure criminal conviction and . . . seldom engages in searches upon a sufficiently regular basis to be affected by the exclusionary sanction." *Id.*; *see also United States v. Janis*, 428 U.S. 433, 455 n.31 (1976) ("[T]he exclusionary rule, as a deterrent sanction, is not applicable where a private party . . . commits the offending act."). Still, "the issue of precisely what it takes to put a search outside the 'private' category is frequently litigated in a wide variety of settings." 1 LaFave, *supra*, § 1.8.

This is one such setting. Windes, on her own volition, searched Phillips's laptop and uncovered child pornography.

While she may not have had the authority to conduct the search on that password-protected laptop, she was clearly acting as a private party. Having discovered child pornography, and thus finding herself in possession of contraband, she decided to take and show it to law enforcement authorities. And when she was informed by a law enforcement officer that she should access the computer so that he could see what she wanted to show him, he made it clear that he did not wish to see anything more than what she had already seen, and she acted in line with those instructions.

1

Phillips asserts that Windes acted as a state agent when she completed the second search because she took cues from Sawyer when doing so. This argument is premised on Sawyer's effort to ensure that in viewing the materials that Windes had already seen and wished to show him, there would be no greater invasion of Phillips's privacy than had already occurred. Because the U.S. Attorney does not dispute Phillips's somewhat counterintuitive assertion that Windes acted as a state agent when she accessed the computer at the sheriff's office, we assume that this was a government search.

Nevertheless, this search was permissible. *United States v. Jacobsen* illustrates "the appropriate analysis of a governmental search which follows on the heels of a private one." 466 U.S. 109, 115 (1984). There, FedEx employees opened a package, saw it contained a white powdery substance, repacked the materials, and alerted the Drug Enforcement Administration ("DEA"). *See id.* at 111. Then, a DEA agent reopened the package, removed its contents without obtaining a warrant, and found that the white powder it contained was cocaine. *See id.* at 111–12. The Supreme

Court held that the FedEx employees' earlier private search and their decision to alert law enforcement to their findings made the agent's warrantless search permissible. The Court explained that "the legality of the governmental search must be tested by the scope of the antecedent private search." *Id.* at 116. "[I]t hardly infringed respondents' privacy for the [DEA] agent to reexamine the contents of the open package" because "the Federal Express employees had just examined the package and had, of their own accord, invited the federal agent to . . . view[] its contents." *Id.* at 119; *see id.* at 120 ("Similarly, the removal of the plastic bags from the tube and the agent's visual inspection of their contents [were permissible actions because they] enabled the agent to learn nothing that had not previously been learned during the private search."). We have thus held that *Jacobsen* establishes that, where a private party notifies law enforcement of its private search, a state "agent's [subsequent] search is permissible, and constitutional, to the extent that it mimic[s the earlier] private search." *United States v. Bowman*, 215 F.3d 951, 956, 963 (9th Cir. 2000).

That is precisely what occurred here. Windes went to the sheriff's office to alert law enforcement to what she uncovered on Phillips's laptop. Sawyer testified that he told Windes to "[j]ust do what you had done and show me what you saw." Windes testified that she "opened up the computer and turned it on, used the same password to log into Phillips'[s] user name, and then opened up the same Phone folder." She then scrolled down and showed him "the same files that [she] saw" the previous night with the same names that she had remembered. *Id.* She "did not access anything that [she] had not previously seen." A video was also admitted into evidence of Sawyer recreating the search he conducted with Windes, which showed that she did not have to "scroll down very far in the 'phone' folder before locating

the thumbnails corresponding to the filenames and descriptions he included in his search warrant affidavit." Based on this evidence, the district court judge found that "Sawyer told [Windes] to not show him anything she had not already seen, she understood his instruction, and she did not show anything she had not already seen." Indeed, the judge "infer[red]" from Sawyer's admonition that "Sawyer was aware of the private search exception and was trying to operate within it."

Although it is possible that—unlike a stagnant container—the folder on Phillips's computer could have automatically updated with new material from his phone between Windes's searches at her home and the sheriff's office or that a previously unviewed notification or alert could have popped up on the screen, Phillips does not allege that his devices were set to do so. Indeed, he concedes that the scope of the two searches was the same. Accordingly, we accept the district court's conclusion that, when Windes accessed the child pornography on Phillips's computer at the sheriff's office, she merely "mimicked [her earlier] private search." *Bowman*, 215 F.3d at 963.[1]

2

Nevertheless, Phillips argues that the evidence uncovered pursuant to Windes's actions at the sheriff's office must be suppressed for reasons tied to law

[1] Even if Sawyer had inadvertently seen more of Phillips's computer than Windes originally had, at least one circuit has held—as then-Judge Sotomayor explained—that "only the information attributable to that *additional* 'search' would require suppression," not the information the private individual already uncovered. *United States v. $557,933.89, More or Less, in U.S. Funds*, 287 F.3d 66, 87–88 (2d Cir. 2002) (Sotomayor, *J.*) (emphasis in original).

enforcement's subjective knowledge. For example, Phillips argues that *Jacobsen* does not apply because: "Sawyer lacked virtual certainty a subsequent search of Phillips's computer would reveal *only* contraband" or "virtual certainty that a subsequent search of the item [would] compromise no remaining privacy interest"; and "Sawyer did not know the details of Windes's [prior] search or full contents of the folder" containing the child pornography before Windes accessed the computer in his presence.[2] Phillips relies on language in the Supreme Court's decision in *United States v. Jacobsen*—language that we repeated in *United States v. Young*, 573 F.3d 711 (9th Cir. 2009). But neither case ultimately supports his arguments.

As Phillips points out, *Jacobsen* states that "[w]hen the first federal agent on the scene initially saw the package, he knew it contained nothing of significance except a tube containing plastic bags and, ultimately, white powder" and that, "[e]ven if the white powder was not itself in 'plain view,' . . . there was a virtual certainty that nothing else of significance was in the package and that a manual inspection of the tube and its contents would not tell him anything more than he already had been told." 466 U.S. at 118–19; *see id.* at 120 n.17 ("[T]he precise character of the white powder's visibility to the naked eye is far less significant than the facts that the container could no longer support any expectation of privacy, and that it was virtually certain that it contained nothing but contraband.").

But read in context, *Jacobsen*'s "virtual certainty" references—and other similar language—do not create any

[2] Phillips argues that, before Windes accessed the computer in Sawyer's presence, she had only told Detective Dickson what she had found and Dickson had not relayed that information to Sawyer.

subjective requirements for the application of its holding. Instead, the language to which Phillips points simply articulates an objective test pertaining to the scope of the searches. The Court described the DEA agent's prior knowledge of the entire package, as conveyed by the Fedex employees, because that knowledge made clear that the package had already been thoroughly examined and thus the government search could not exceed the scope of those employees' prior one. Indeed, the Court went on to explain:

> Respondents do not dispute that the Government could utilize the Federal Express employees' testimony concerning the contents of the package. If that is the case, it hardly infringed respondents' privacy for the agents to reexamine the contents of the open package by brushing aside a crumpled newspaper and picking up the tube. The advantage the Government gained thereby was merely avoiding the risk of a flaw in the employees' recollection, rather than in further infringing respondents' privacy. Protecting the risk of misdescription hardly enhances any legitimate privacy interest, and is not protected by the Fourth Amendment.

Id. at 119. The Court's explanation confirms that a government search that does not exceed the bounds of a private one is not an invasion of privacy under the Fourth Amendment. The only advantage gained by the government's own search is avoiding the private party's "misdescription"—and that is a permissible advantage. What was important to the *Jacobsen* Court was that the DEA agent's search "enabled [him] to learn nothing that had not previously been learned during the private search," not that

he have subjective knowledge of what was learned during the private search. The description of the DEA agent's knowledge simply made clear that he was not exceeding the private search. *Id.* at 120; *see also id.* at 116 ("[T]he legality of the governmental search must be tested by the scope of the antecedent private search."). "As in other Fourth Amendment contexts," then, the inquiry remains "an objective one." *Graham v. Connor*, 490 U.S. 386, 397 (1989); *cf. Torres v. Madrid*, 141 S. Ct. 989, 998 (2021) ("[W]e rarely probe the subjective motivations of police officers in the Fourth Amendment context.").

Here, as in *Jacobsen*, Windes's accessing the computer in Sawyer's presence "enabled [Sawyer] to learn nothing that had not previously been learned during the private search" and was therefore permissible. *Id.* at 120. But unlike *Jacobsen*, our conclusion regarding the equivalence between the scope of the searches arises because the record demonstrates that Sawyer instructed Windes to recreate her prior search so he only saw what she had already seen, and Windes abided by those instructions.[3]

Our opinion in *Young*, 573 F.3d 711, does not change this conclusion. It simply represents an application of the Supreme Court's decision in *Stoner v. California*, 376 U.S. 483 (1964). *Stoner* held that "[n]o less than a tenant of a

[3] Moreover, even if *Jacobsen*'s application depends on the subjective knowledge of the person conducting the search, that test was satisfied here. Unlike the DEA agent in *Jacobsen*, who had not conducted the initial search but who had learned about the entire contents of the package from the FedEx employees, Windes had previously accessed the Phone folder of Phillips's computer and saw that it contained child pornography. Thus Windes—the alleged state agent conducting the subsequent search in this case—possessed subjective knowledge and virtual certainty of what her search would reveal.

house, . . . a guest in a hotel room is entitled to constitutional protection" from a warrantless entry into his room regardless of any prior intrusion or permission given by hotel employees. *Id.* at 490. In *Young*, hotel security initially entered the defendant's room without his permission to investigate whether he had stolen items from another guest, and they uncovered a gun in his backpack in addition to other items. 573 F.3d at 714. This was a private search that did not implicate the Warrant Clause of the Fourth Amendment. Nevertheless, the issue in *Young* turned on a second entry into and search of the hotel room by hotel security after they contacted law enforcement officers. *Id.* at 715. "The Government d[id] not dispute the district court's conclusion that [hotel] security should be considered state actors for the purposes of the second search." *Id.* at 717. Thus, *Young* involved a warrantless entry into the defendant's hotel room by state actors against which he was protected by the Warrant Clause because "a hotel guest's . . . room is like a home . . . [and the] guest has a legitimate and significant privacy interest . . . against unlawful government intrusions." *Id.* at 721. And, absent exigent circumstances, such an intrusion is unlawful if undertaken without a warrant or consent of the occupant. *See Stoner*, 376 U.S. at 489–90; *see also Payton v. New York*, 445 U.S. 573, 589–90 (1980) ("[A]t the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion. . . . Absent exigent circumstances, that threshold may not reasonably be crossed without a warrant." (alterations and internal quotation marks omitted)).

The language in *Young* upon which Phillips relies appears in our discussion rejecting "[t]he Government['s] argu[ment]," which it had raised "for the first time on appeal, that *United States v. Jacobsen* . . . should be extended to

permit the search of Young's backpack stored in his hotel room." 573 F.3d at 720. Phillips is correct that in *Young* we discussed language from *Jacobsen* that, by the time the DEA agent arrived, "it was virtually certain that [the package] contained nothing but contraband." *Jacobsen*, 466 U.S. at 120 n.17; *see Young*, 573 F.3d at 721. But when we did so, it was merely to explain that *Young* "[wa]s distinguishable from *Jacobsen" because the hotel security* "could not have been 'virtually certain' . . . that the gun was contraband." *Id.* After all, unlike narcotics, "[i]t is not a crime in most circumstances for a non-felon to possess a gun." *Id.*

While the two cases were distinguishable in the manner *Young* suggested, it is unlikely this distinction was crucial to our decision. Surely, we did not mean to suggest that our decision would have been different had the hotel security in *Young* been "virtually certain" as to the nature of the items the second search of Young's hotel room would uncover. Indeed, it could not have been. Unlike this case, *Young* concerned the unique privacy interests an individual has in his residence (and, by extension, a temporary residence like a hotel room). *See United States v. Lichtenberger*, 786 F.3d 478, 484 (6th Cir. 2015) ("Homes are a uniquely protected space under the Fourth Amendment."). Under *Stoner*, no prior private search and no level of certainty regarding what the second search would uncover could have allowed state actors to enter Young's hotel room without a warrant or his consent. *Young* relied expressly on well-settled Supreme Court law that "[b]elief, *however well founded*, that an article sought is concealed in a dwelling house, furnishes no justification for a search of that place without a warrant. And such searches are held unlawful notwithstanding facts unquestionably showing probable cause." 573 F.3d at 721 (emphasis added) (quoting *Johnson v. United States*,

333 U.S. 10, 14 n.14 (1948))).[4] Unlike *Young*, but like *Jacobsen*, this case does not involve a warrantless entry into a home or its equivalent. Accordingly, *Young* does not alter the current inquiry.

Phillips also argues that the extensive amount of personal information contained in a laptop makes it similar to a private residence, meaning that the private search doctrine should not apply. An analysis of this argument depends on to which of the two aspects of the doctrine it refers. The first involves an intrusion—even an extraordinarily invasive intrusion—by a private party who gives the contents discovered pursuant to that intrusion to law enforcement. *Burdeau v. McDowell*, 256 U.S. at 475–76. The validity of this conduct does not depend on the extent of the private information contained in the object or location on which the private party intruded. If there is no state action, there is no Fourth Amendment violation. *Id.*

By contrast, the second aspect of the private search doctrine involves "a governmental search which follows on the heels of a private one," *Jacobsen*, 466 U.S. at 115, and it is to this aspect of the doctrine that Phillips's argument refers. While it is true that modern computers contain so much personal information that a search of one could

[4] The leading treatise on the Fourth Amendment cites *Young* correctly for the proposition that "it is to be doubted that if a private person searched the premises of another and then reported to police what he had found . . . that the police could then make a warrantless entry of those premises and seize the named evidence." 1 LaFave, *supra*, § 1.8(b) & n.97. Indeed, *Young* was guided by the analytic framework of the Sixth Circuit in *United States v. Allen*, 106 F.3d 695, 698–99 (6th Cir. 1997), which specifically rejected the argument that *Jacobsen* could permit a "warrantless search of [a defendant's] motel room." *See Young*, 573 F.3d at 720–21.

"expose to the government far *more* than the most exhaustive search of a house," *Riley v. California*, 573 U.S. 373, 396 (2014), and more than the private party had previously uncovered, we have already held that the private search doctrine does apply to them, *see United States v. Tosti*, 733 F.3d 816 (9th Cir. 2013). We note that unlike in *Riley*, which involved a search incident to arrest, the search here involved a clear limiting principle: the private search exception allows police to review only the material that a private actor has already viewed. Because a digital container like "an email account, cell phone, or laptop" is composed of many smaller containers, a subsequent government search of a single file (or even a number of files) will not frustrate an individual's privacy interest in the entire device. *United States v. Wilson*, 13 F.4th 961, 977 n.13 (9th Cir. 2021). We acknowledge that it may be more difficult to have "virtual certainty" that a search of an electronic device does not reveal more than the private search had already revealed, given the dynamic nature of such devices. *See United States v. Rivera-Morales*, 961 F.3d 1, 13 (1st Cir. 2020) ("The Court did not define 'virtual certainty,' and it is not immediately apparent how that concept translates from the context of a static object like a package to the ever-changing screen on a cellphone."); *see also Lichtenberger*, 786 F.3d at 488. In this case, however, all parties agree that the officer did not see anything more than Windes had previously viewed, so we need not address this issue.

3

Phillips additionally argues that the Supreme Court's decision in *United States v. Jones*, 565 U.S. 400 (2012), supports reversing the district court's decision. In *Jones*, police attached a GPS tracking device to a car owned by the defendant's wife without a valid warrant. *Id.* at 402–03. The

district court denied the defendant's motion to suppress the data the police collected from that device, holding that the defendant lacked a reasonable expectation of privacy with respect to the car's movements on public streets. *Id.* at 403. The Supreme Court disagreed. It explained that, even if the defendant lacked a reasonable expectation of privacy with respect to the car's public movements, the Fourth Amendment nonetheless prohibited the police from physically trespassing on the defendant's wife's car by installing and using the tracking device without a valid warrant, and the exclusionary rule applied to the fruits of that unwarranted trespass. *Id.* at 404–06.

According to Phillips, *Jones*'s "common-law trespassory test" for Fourth Amendment violations requires suppression in this case. *Id.* at 409. *Jacobsen*, Phillips says, merely stands for the proposition that a private search eliminates an individual's reasonable expectation of privacy with respect to an item's contents. Thus, the fact that Windes had previously viewed the files containing child pornography on Phillips's computer only eliminated his reasonable expectation of privacy with respect to those files. It did not, Phillips argues, give Sawyer the license to instruct Windes to again "physically intrude[]" on Phillips's property—*i.e.*, his computer—by "open[ing] the laptop computer, enter[ing] the password . . . navigat[ing] to the 'phone folder' and scroll[ing] through the images." And, under *Jones*, that intrusion violated Phillips's Fourth Amendment rights.

This argument fails. Even if we attribute Windes's action to the officers and assume that those actions constituted a "trespass" of Phillips's property, *Jacobsen*, too, involved a trespass of the defendant's property. There, after the FedEx employees had opened the defendant's package and found

white powder, the DEA agent reopened the package and removed its contents. Yet the Supreme Court permitted the warrantless search even though the agent physically intruded onto the package. *See Jacobsen*, 466 U.S. at 118–22. *Jacobsen* thus establishes that law enforcement officers do not violate the Fourth Amendment when, as Phillips claims occurred here, they mimic the trespass a private individual visited on another's possessions after being alerted to the information uncovered pursuant to that trespass. *See Bowman*, 215 F.3d at 956, 963. *Jones* did not involve any aspect of the private search exception, nor did it reference *Jacobsen*. Under these circumstances, we must follow the Supreme Court's instruction that "if a precedent of this Court has direct application in a case, yet appears to rest on reasons rejected in some other line of decisions, the Court of Appeals should follow the case which directly controls, leaving to this Court the prerogative of overruling its own decisions." *Agostini v. Felton*, 521 U.S. 203, 237 (1997) (internal quotation marks and citation omitted).

Moreover, our decision in *Tosti*, which postdates *Jones*, is consistent with our rejection of Phillips's argument. There, a computer technician uncovered child pornography on the defendant's computer and alerted the police. *Tosti*, 733 F.3d at 818–19. When two detectives arrived, without first obtaining a warrant, one of them "directed [the technician] to open the images in a 'slide show' format so that they would appear as larger images viewable one by one." *Id.* at 819. The technician then "opened up the individual images" as the detective requested. *Id.* We held that, in light of the technician's prior search, *Jacobsen* dictated that these actions did not violate the defendant's Fourth Amendment rights. *Id.* at 821–22. Thus, we applied *Jacobsen* even though the technician, at the "direct[ion]" of the detective, arguably physically intruded on the defendant's computer

when he "opened up the individual images." *Id.* at 819. If *Jacobsen* applied in *Tosti*, it must also apply here.

Indeed, this case may be a stronger case than *Tosti* for applying *Jacobsen*. When Windes, acting as a private person, discovered the child pornography on Phillip's computer, she had at least two options for bringing it to the attention of law enforcement. First, and impracticably, she could have entered the sheriff's office with laptop open and the child pornography displayed in plain view. Second, she could have entered with the laptop closed and waited until she was in a private setting before opening the laptop and navigating to the child pornography. Sensibly, she chose the second option. And the only direction she received from a law enforcement officer was aimed at ensuring that she would not intrude on Phillips' privacy more than she already had.

In *Coolidge v. New Hampshire*, the Supreme Court observed in analogous circumstances that had the defendant's wife "wholly on her own initiative, sought out her husband's guns and clothing and then taken them to the police station to be used as evidence against him, there can be no doubt under existing law that the articles would later have been admissible in evidence." 403 U.S. at 487 (citing *Burdeau*, 256 U.S. 465). Phillips argues that because Windes chose the second option, the evidence uncovered pursuant to her actions at the sheriff's office must be suppressed. "[I]t would seem strange" if the result in "cases of this kind . . . [would] 'turn on the fortuity' of whether and to what extent the private person put the contents back into [or closed] the container before the police appeared," 1 LaFave, *supra*, § 1.8(b) (quoting *Jacobsen*, 466 U.S. at 120 n.17).

Tosti's application of *Jacobsen* to permit "the warrantless searches of [the defendant's] computer," *id.* at

821–22, also disposes of Phillips's argument, which we have already addressed, that "given the significant privacy interests implicated by modern digital devices, [*Jacobsen*] is categorically inapplicable to warrantless searches of these devices, such as Phillips's personal computer." *Cf. United States v. Wilson*, 13 F.4th 961, 972 (9th Cir. 2021) (declining to extend *Jacobsen* to a case where, in response to a Google report that its algorithm detected a match between images the defendant had attached to an email and known child pornography, "the government agent viewed [the] email attachments even though no Google employee—or other person—had done so"). Other circuits have also applied *Jacobsen* to searches of modern digital devices. *See United States v. Castaneda*, 997 F.3d 1318, 1327–29 (11th Cir. 2021); *Rivera-Morales*, 961 F.3d at 8–11; *United States v. Reddick*, 900 F.3d 636, 638–39 (5th Cir. 2018); *Lichtenberger*, 786 F.3d at 483–84; *United States v. Goodale*, 738 F.3d 917, 921 (8th Cir. 2013); *Rann v. Atchison*, 689 F.3d 832, 836–37 (7th Cir. 2012).

Phillips's objections to the use of evidence obtained from his computer therefore all fail.

We also reject Phillips's challenge to three conditions of his supervised release. Because Phillips signed a valid appeal waiver, he may argue on appeal only that those conditions "exceed[] the permissible statutory penalty [for the crime] or violate[] the Constitution." *United States v. Watson*, 582 F.3d 974, 981 (9th Cir. 2009). Yet our precedents establish the legality of all the challenged conditions. *See United States v. Gibson*, 998 F.3d 415, 422–23 (9th Cir. 2021) (risk notification), *cert. denied*, No. 21-6465 (Jan. 10, 2022); *United States v. Ochoa*, 932 F.3d 866, 869–71 (9th Cir. 2019) (prohibiting access to material depicting sexually explicit conduct involving adults to

defendant convicted of child pornography offense); *United States v. Stoterau*, 524 F.3d 988, 1003–04 (9th Cir. 2008) (polygraph testing).

The judgment of conviction is **AFFIRMED**.